Please replace the paragraph beginning on page 21, line 9 with the following rewritten paragraph:

(S62) The CPU 2, if the data in the region L1 have not been read out, executes the process of developing the key data in the operation region of the memory 3. Namely, the CPU 2 obtains the user password Pwi. Then, the CPU 2 reads the data from a region Li and decodes the read data with the password Pwi. The password PW1 is thereby obtained on the optical disk 1.

In the Claims:

Please amend claims 1, 3, 7, 8, 10, 14 and 15 and add new claims 16-19 as follows:

1. (Amended) A storage medium data protecting method of protecting data on a storage medium, comprising:

a step of generating key data, encrypting the key data with a password, and writing the encrypted key data to said storage medium;

a step of encrypting the data with the key data, and writing the encrypted data to said storage medium;

a step of reading the encrypted key data from said storage medium;

a step of decoding the encrypted key data with the password; and

a step of decoding the data on said storage medium with the decoded key data,

wherein said key data generating step comprises a step of generating different key data for each of a plurality of unit storage areas of said storage medium.

3. (Amended) A storage medium data protecting method according to claim 1, wherein said key data generating step comprises a step of generating is different key data for each writing to said unit storage areas.

7. (Amended) A storage medium data protecting method according to claim 1, wherein said step of writing the encrypted key data to said storage medium comprises a step of encrypting the key data with a first password, writing the encrypted key data to said storage medium, encrypting a second password with said first password, and writing said second encrypted password, and

said step of decoding the key data comprises a step of decoding said second encrypted password with said second password, and obtaining said first password, and a step of decoding the encrypted key data with said first password.

8. (Amended) A storage medium data protecting apparatus for protecting data on a storage medium, comprising:

a storage medium having a plurality of unit storage areas; and

a control circuit for reading and writing the data from and to said storage medium,

wherein said control circuit has:

a write mode of encrypting, after generating key data, the key data with a password, writing the encrypted key data to said storage medium, encrypting the data with the key data, and writing the encrypted data to said storage medium;

a read mode of encoding, after reading the encrypted key data from said storage medium, the encrypted key data with the password, and decoding the data on said storage medium with the decoded key data,

wherein said key data comprises different key data for each unit storage area of said storage medium.

10. (Amended) A storage medium data protecting apparatus according to claim 8, wherein said control circuit generates different key data for each writing to said unit storage areas.

14. (Amended) A storage medium data protecting apparatus according to claim 8, wherein said control circuit has:

a write mode of encrypting the key data with a first password, writing the encrypted key data to said storage medium, encrypting a second password with said first password, and writing said second encrypted password; and

a read mode of decoding said second encrypted password with said second password, obtaining said first password, and thereafter decoding the encrypted key data with said first password.

15. (Amended) A storage medium having protected data is stored with;

a plurality of key data encrypted with a different password data for each of a plurality of unit storage areas of said storage medium; and

data encrypted with the different key data for each said unit storage area of said storage medium.

16. (New) The storage medium protecting method according to claim 1, said writing the encrypted key data step is performed for all unit storage areas of said storage medium when initializing said storage medium.

17. (New) The storage medium protecting method according to claim 16, said encrypting the data step comprises:

a step of reading the encrypted key data from said storage medium;

a step of decoding said read encrypted key data with said password; and

a step of encrypting the data with said decoded key data.

18. (New) An encoding method protecting data on a storage medium, comprising:

a step of generating different key data for each unit storage area of said storage medium, encrypting the key data with a password, and writing the encrypted key data to said storage medium;

a step of encrypting the data with the key data, and writing the encrypted data to said storage medium.

19. (New) A decoding of protected data on a storage medium, comprising:

a step of reading the encrypted key data which is encrypted with different key data for each unit storage area of said storage medium from said storage medium;

a step of decoding the encrypted key data with the password; and

a step of decoding the data on said storage medium with the decoded key data.

REMARKS

Attached hereto is a marked-up version of the changes made to the specification and claims by the current amendment. The attached page is captioned "**Version with markings to show changes made.**"

As a preliminary matter, applicants request acknowledgement of the JP '021 reference filed with an Information Disclosure Statement on October 20, 2000. A copy of the 1449 form filed with that IDS is attached.